

UNITED STATES DISTRICT COURT

for the
District of New Mexico

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Dell Precision m4800 Laptop Computer, serial number
F27TF12, located at the New Mexico State Police
Evidence Vault, 2501 Carlisle Blvd NE, Albuquerque, NM

Case No. 16-MR-36

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Dell Precision m4800 Laptop Computer, serial number F27TF12, currently located at the New Mexico State Police Evidence Vault, 2501 Carlisle Blvd NE, Albuquerque, NM 87110

located in the _____ District of _____ New Mexico _____, there is now concealed *(identify the person or describe the property to be seized)*:

Dell Precision m4800 Laptop Computer, serial number F27TF12

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C § 666Offense Description
Theft or Bribery concerning Programs Receiving Federal Funds

The application is based on these facts: See Attachment

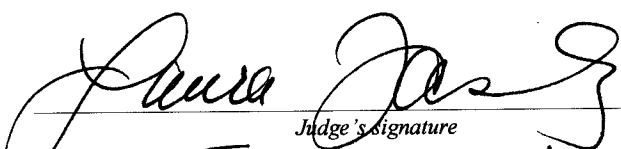
☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

 Applicant's signature
Jaime Ordonez, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/13/2016

City and state: Albuquerque, NM


 Judge's signature
Laura Fashing, U.S. Magistrate
Printed name and title

Judge

IN THE UNITED STATES DISTRICT COURT
FOR NEW MEXICO

IN THE MATTER OF THE SEARCH OF
DELL PRECISION m4800 LAPTOP
COMPUTER S/N:F27TF12, CURRENTLY
LOCATED AT THE NEW MEXICO STATE
POLICE EVIDENCE VAULT, 2501
CARLISLE BLVD NE, ALBUQUERQUE,
NM 87110

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Jaime Ordonez, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security (DHS), Office of Inspector General (OIG), El Paso, TX, and have been since January 2008. Prior to DHS OIG your affiant was employed as a Special Agent with the Drug Enforcement Administration (DEA) from July 2000 to December 2007. Affiant has received specialized training in criminal investigations through the Federal Law Enforcement Training Center, the Inspector General Criminal Investigator Training Academy, the DEA Training Academy and Public Agency Training Council. Affiant has received classroom and on the job training. Affiant has specialized training and experience in the area of financial crimes and the investigation of contract fraud and

other criminal violations. Affiant has conducted numerous criminal investigations that have led to the arrest and conviction of persons in violations of federal criminal statutes.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a Dell Precision M4800 laptop computer, serial number F27TF12, hereinafter the "Device." The Device is currently located at the New Mexico State Police Evidence Room, 2501 Carlisle Blvd NE, Albuquerque, NM 87110.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. In September 2015, the Department of Homeland Security Office of Inspector General received an allegation that the New Mexico Task Force I (NM-TF1), which is part of the Federal Emergency Management Agency (FEMA) Urban Search and Rescue team, located in Albuquerque, NM, produced and provided fraudulent training certificates showing that its task force members had completed FEMA's on-line introductory ethics training course. When the provided certificates were checked against the FEMA's Emergency Management Institute database, the information revealed that the courses had not been completed and/or the dates differed from the information on the database. The fraudulent certificates were provided to FEMA by NM-TF1 in order to receive federal program funds and to certify NM-TF1 in order for them (NM-TF1) to respond to disaster areas. As the investigation proceeded a source of

information (SOI) came forward and provided information. The identity of the SOI is known to me, and based on the totality of the circumstances in the investigation to date, I believe the information provided by the SOI to be reliable. The SOI who works for NM-TF1 said that he/she was tasked with assisting Dante Halleck, the former training manager for NM-TF1, with getting the task force in compliance with training requirements in order for NM-TF1 to be able to deploy to disaster areas and receive its yearly funding from FEMA. The SOI stated that as he/she started going through the training folders of the task force members he/she observed that many members lacked the FEMA ethics training. The SOI then approached Halleck and made him aware of the lack of training certificates. Halleck responded that he was in possession of a FEMA certificate template, that Halleck obtained from a person in Santa Fe, NM, and that he would manufacture the training certificates. Halleck then asked the SOI for names of persons who were lacking the ethics training and proceeded to input the names into the Device (Dell Precision M4800 laptop computer) and print out a fraudulent certificate to be placed in the training file.

7. The SOI stated that he/she witnessed Halleck print out numerous fraudulent training certificates. The SOI then stated that besides the fake ethics training certificates, a second review of the personnel files revealed fraudulent certificates for fit tests, hazmat tests and respiratory certificates. After a FEMA led audit of the NM-TF1, the SOI stated that all the fraudulent certificates were removed from the personnel files and secured as evidence. Additionally, the SOI stated that Halleck's laptop computer was secured and all items were turned over to Jay Mitchell, Cabinet Secretary, State of New Mexico. Jay Mitchell subsequently turned over the items to the New Mexico State Police Department.

8. Based on the facts stated above, there is probable cause to believe that evidence, fruits or instrumentalities of the offense of theft from programs receiving federal funds, 18 U.S.C. Section 666, will be found within the Device.

9. NM-TF1 is a team of state sponsored employees who receive funding and technical direction on standard operating procedures, equipment, training, and exercise requirements from the Federal Emergency Management Agency Search and Rescue Program, to assist in disaster related operations. The task force had been out of compliance for several years due to a majority of its task force members not meeting FEMA's training standards and/or certification requirements. However, FEMA continued to fund NM-TF1 in order for NM-TF1 to attain compliance and certify its task force members to deploy to disaster areas.

10. The Device is currently in the lawful possession of the New Mexico State Police. It came into the New Mexico State Police possession in the following way: The New Mexico State Police took possession of the device from Jay Mitchell, Cabinet Secretary, State of New Mexico who took possession of the device from Jim Tuma, Interim Training Manager, New Mexico Task Force I, Urban Search and Rescue, who had taken possession/seized the Device from Dante Halleck and held as evidence. Therefore, while the New Mexico State Police might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

11. The Device is currently in storage at the New Mexico State Police Evidence Vault. In my training and experience, I know that the Device has been stored in a manner in

which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the New Mexico State Police.

TECHNICAL TERMS

12. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Laptop Computer: A laptop computer is a portable computer light and small enough to sit on a person's lap. A laptop computer can be powered by battery or plugged into the wall. The main utility of a laptop computer is that it allows a person to travel with their computing resource.

13. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a mobile workstation which contains an i5-4210 Processor, 8 gigabytes of memory, 500 gigabyte hard drive and an intel dual band wireless Bluetooth and mini card. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

14. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via electronic mail or the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

15. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but

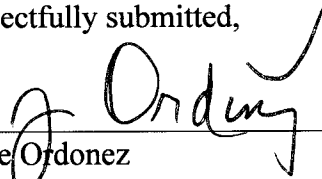
not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

18. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.


CONCLUSION

19. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Jaime Ordonez
Special Agent
Department of Homeland Security
Office of Inspector General

Subscribed and sworn to before me
on January 13, 2016 ~~January 14, 2016~~: 



UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a Dell Precision M4800 laptop computer, serial number F27TF12, hereinafter the "Device." The Device is currently located at the New Mexico State Police Evidence Room, 2501 Carlisle Blvd NE, Albuquerque, NM 87110.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C § 666 (Theft or Bribery concerning Programs Receiving Federal Funds) and involve Dante Halleck since August 2014, including:
 - a. All records contained in electronic and/or digital, magnetic and/or optical media and/or device(s) including the computer hard disc drive(s), computer network hardware, and any removable electronic storage device in the computer capable of creating, analyzing, displaying, converting, storing and/or transmitting electronic and/or digital, magnetic and/or optical impulses and/or data, that relate to Dante Halleck's creation of fraudulent training certificates and other efforts to obtain FEMA funds without complying with FEMA regulations. Any and all instructions and/or programs that can be interpreted by a computer or related components. Any and all application software, operating systems, utility programs, compilers, interpreters and/or other programs and/or software used to communicate, directly and/or indirectly, with computer hardware and/or peripheral computer device(s). This warrant shall authorize the complete search, to include but not limited to, the copying and viewing, of said computer and/or devices, to be searched. It may be necessary to seize said media and/or device(s), whole or in part, for subsequent analysis.
 - b. Any record documented on any media, which appears to list and/or identify e-mail addresses, e-mail messages/correspondences, internet sites, user names, user identification numbers, internet provider information, writings, or

fz go.

communication, including ~~but not limited to~~, letters, instant messages, or any type or correspondence which describes, displays images, or contains information or acts, memos in whole or in part, that relate to Dante Halleck's creation of fraudulent training certificates and other efforts to obtain FEMA funds without complying with FEMA regulations. This warrant shall authorize the complete search, to include but not limited to, the copying and viewing, of the said media and/or devices, to be searched. It may be necessary to seize the herein-described media and/or device(s), whole or in part, for subsequent analysis.

- c. Any record documented on any media, which appears to be a password, personal identification number, item(s) and/or information used to access and/or facilitate access of said item(s), to be searched.
- d. Any record documented on any media, which establishes and/or tends to establish the state of mind, motive(s), action(s), means and/or intention(s) of any person(s) with knowledge or apparent knowledge of the crime(s), including diaries, journal(s) audio and/or video recordings.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.